

## An enhanced security alert system for smart home using IOT

Afshana Khanum<sup>1</sup>, Rekha V<sup>2</sup>

<sup>1</sup>Department of Computer Science &Engineering, SJB Institute of Technology, India

<sup>2</sup>Department of Computer Science & Engineering, Faculty of Engineering, Christuniversity, India

---

### Article Info

---

#### **Article history:**

Received Jul 11, 2018

Revised Sep 12, 2018

Accepted Sep 26, 2018

---

#### **Keywords:**

IOT

Mobile IP webcams

RaspberryPi

Smart home security

Socket

Wi-Fi

---

### ABSTRACT

---

Today due to advancement in technology and Internet of Things, to deal with step-by-step jobs like mailing, accessing bank entries, watching degree of hotness and other jobs PCs were utilized. Because of fast improvement in IOT nowadays tablets, advanced mobile phones are utilized for such assignments [1]. Home security can be characterized as observing the home remotely located or centrally located. Today, home security is getting to be vital as the conceivable outcomes of interruption is expanding step by step, yet they have issues like postponement, non-web empowered and hard to deal. Intruder recognition is basic parts of home computerization and home security frameworks. Most generally, utilized specialized devices are mobile phones and sending mails are considered for controlling home appliances remotely by proposing productive structures. An Enhanced Security Alert System for Smart Home using IOT is composed in our proposed work. It identifies the intruder when no one is in home by sending alert message or caught picture to the proprietor (or) owner. Proposed framework is ease home security framework utilizes an IP Web-camera and Raspberry pi for limiting delay during the time of sending alert message. Fog Computing is incorporated to proposed framework to expand the level of security and limit the engendering delay. Proposed framework is to give minimal effort arrangement and adape association instrument for coordinating Internet of Things with home security frameworks.

*Copyright © 2019 Institute of Advanced Engineering and Science.  
All rights reserved.*

---

#### **Corresponding Author:**

Afshana Khanum,  
Department of Computer Science &Engineering,  
SJB Institute of Technology, india.  
Email: khanumafsha@gmail.com

---

### 1. INTRODUCTION

Today, each device is connected with the help of internet. The interconnection of devices like sensors installed with hardware empowers the things to gather information over internet. Hence, Internet of things (IoT) is basically the system of interconnected devices which are implanted with sensors, programming, network connectivity and important hardware that empower to gather and trade information making them responsive without expecting that human-should human or human-to PC cooperation [2]. In today's communication technology, communication is not only done between computers, but it completely done over a network and is called network. With advance internet technology not only, we can access data at any place, any person, any time but also can be control and monitor at any place, any time and this special technology is called as Internet of Things (IoT) [3]. An incredible increasing portion of the extension in IoT communication begins from enrolling devices and embedded sensor structures used as a part of mechanical machine-to-machine (M2M) communication, home and building robotization, vehicle-to-vehicle communication and wearable processing devices.

Security means safety, as well as the measures taken to be safe or protected. To improve security, an IoT device that should need to be specifically open over the Internet, ought to be divided into its own system

and have network access limited. Security in IOT is the zone of effort worried about safeguarding related gadgets/devices and frameworks in the Internet of things (IoT) [4].

IoT security ruptures are ascending in private applications. The way that few end customers find a way to guarantee security, for example, refreshing firmware, proposes that numerous don't organize prioritize issues. These components may clarify why end customer are extremely reluctant to pay for enhanced security. Numerous companies have endeavoured to set up security standard for keen home IoT applications, including OEMs, Internet players, and tech companies [5]. The companies that wind up predominant that become dominant within the nascent sector should prevail in setting standards, but it is not yet clear which these will be. Smart home security could pick up footing if engineers interface it with another element that customer value, for example, ease of use. For instance, innovations or arrangements that significantly streamline setup endeavours and increment security could be sought after. Since numerous smart home devices have short substitution cycles, and since they require a restricted speculation for every family, the market could encounter solid development if stimulates by major event. To profit by this pattern, semiconductor organizations should put down their wagers now on the brilliant home biological communities that will wind up predominant. IoT network security is more demanding than traditional system security in light of the fact that there is a more extensive scope of communication protocols, and gadget abilities, all of which posture significant issues and increased complexity. Key capabilities incorporate network endpoint security features, for example, antivirus, antimalware, and additionally different highlights, for example, firewalls and intruder detection and prevention system [1]. Also, obviously, not all IoT frameworks have a similar security necessity, however for a large number of them security implies safety and such frameworks should be focus [1].

## 2. RELATED WORK

Some existing works on Enhance IOT based Security Alert System for Smart Home Farrukh Shahzad et al. [2] have proposed a minimal effort answer for interruption insurance which has a short alarm time and is nearly fall flat evidence is displayed. An application utilizing the vicinity sensor of a cell phone is created to show that our homes also, different properties can be secured against interruptions without spending a great many dollars in surveillance cameras and security monitors. Test comes about demonstrate that advanced mobile phones are not just equipped for identifying a gatecrasher all alone however can likewise advise the property proprietor of the interruption close to interruption with the goal that unexpected move can be made and, in this manner, assets can be spared from being stolen.

K. Balasubramanian et al. [3] proposed home automation security alert system, which can control the home appliances remotely and alert the owner whenever intruder occurs in the home. It includes intruder detection using LDR and Sensor circuits.

Akshat Jain, Shraddha Basantwan, OwaisKaz, Yogita Bang et al. [6] have proposed, thought of an answer of brilliant surveillance system for particular spots like bank vaults, homes where the human closeness isn't available. At such places, it isn't worth to reliably screen the area with the cameras. This squanders the power use and the limit required for the recordings. Our framework will recognise human nearness using PIR sensor. Raspberry Pi works and controls development recognising sensors and camcorders for remote identifying and perception, streams live video and records it for future playback. On distinguishing proof of any improvement the cameras will trigger the observation. The proposed framework gets information and transmits it by methods for Internet to mobile phones and workstations. Live spouting is done all through the WAN i.e. also open inside different LANs. Wide human observing of the approach video channels is irrational, expensive and inadequate. Using a general test based foundation subtraction computation called ViBe (Visual Background Extractor), we identified development in red alert zone i.e. a place in the room where the assets are set, for any suspicious development and we send an alarm to the customer. The video recorded and set away can be used to perceive the gatecrasher and help in getting him. To shield assurance and securely transmit the video film over the framework, we are using blowfish encryption and unscrambling figuring to give extra security from developers.

Ayush Panwar and Anandita Singh et al. [7] proposed open source and cost effective and secure home portraying the utilization of open source equipment like Arduino, Raspberry pi, Arm processor and so forth. It clarifies how a computerized home can be observed (or) controlled utilizing Google voice charges.

Mehdi Nobakht et al. [8] proposed intruder detection system to provide network level security deployed for home appliances deployed in smart home environments. Smart devices are gaining fame in our homes with the guarantee to make our lives less demanding and more agreeable. This system is also capable of blocking the intruder in accessing victim device.

Supreetavenkatesan et al. [9] focuses on designing and developing a model of security alert system for, banks. Security has become major these days especially in the rate of crimes. Research shows that homes

without security are targeted with intruder than professionally monitored homes. This system is for detecting intruder and sends alert to the user through text message. And also, it is less power consumption compared to existing system as the camera is activated and takes snapshots only when an intruder is detected. And it not only notifies to the owner also to neighbour so that immediate action could be taken.

Umesh Chandra Pati et al. [10] talk about the use of PIR sensors in such frameworks and utilization of Zig Bee to make the safe home. These days the need of building compelling interruption recognition framework is fundamental as plausibility of gatecrasher assault expands step by step. GSM module is utilized to catch the picture and send ready message to the proprietor at whatever point interloper go into the home. PIR sensor, being latent in nature is imperceptible and function admirably oblivious condition. Distinctive sensor hubs, which utilize Zig Bee for remote transmission, are altogether associated with a middle hub. Effectively monitor the movement information and interface with get to organize administrator for getting client's SLA and mastermind ahead of time assets according to. What's more change in SIP welcomes and re-welcome message to incorporate asked for data was utilized. These progressions will be useful in ensure accessibility of client's handset capacity to IMS centre system.

Vishal Jain et al. [11] focus on building smart security system which alerts the owner by raising an alarm sound. Along with this it can make use of making home automated by using same sensors. The electrical devices inside the house can be controlled and manage by using microcontroller a current prototype- TI-CC3200.

Break in literature survey stimulate us to increase the level of security for society, so that people in the society can live without tension. The work in this paper is carried out to reduce the society robbery as well as in future it can be implemented for banks, etc. An enhanced security alert system s designed so that when nobody is in home the system will recognise home relative or intruder and sends an email alert so that owner can feel relax when he (or) she will out of the home. And this will be helpful for the society. The rest of the papers have the following section

- a) Section 4 - Architecture model
- b) Section 5 - Problem statement & Results
- c) Section 6 - Conclusion

Research of this paper includes the

- a) Review on internet of things.
- b) Various results are identified for detecting intruder.
- c) Proposed architecture is low cost for detecting intruder using Raspberry pi.

### 3. AN ENHANCED SECURITY ALERT SYSTEM FOR SMART HOME USING IOT

#### 3.1. Outline

In this work, an enhanced IoT based Security Alert System for Smart Home is Proposed in order to detect an intruder or any unusual event occur in the home, in the absence of home owner (or) person.

Figure 1 depicts the block diagram of the IoT based Security Alert System. It consists of 3 steps. In step 1, live video will be collected through mobile webcam has frames and emitted. In step 2, collected sample frames are compared to match registration samples [2]. Here, the standard of collected samples is improved with the registered sample. In step 3, finally, it notifies if the samples mismatch with the registered module then an email alert will be send to the owner and action will be taken. Section 4.2 presents algorithm of Security Alert System with respect to Smart Home.

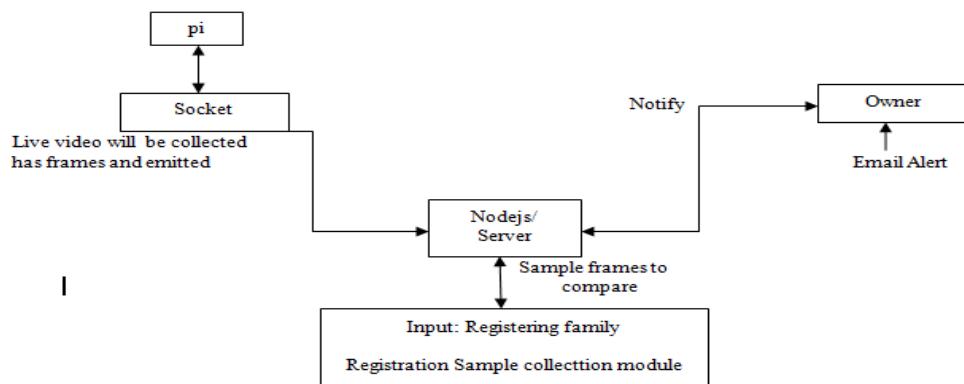


Figure 1. Architecture of security alert system

### 3.2. Experimental Setup

In this proposed System we have considered two phases:

- First phase explains about the hardware components used.
- Second phase says about algorithm and email alert procedure sending to homeowner.

Following is the description provided for hardware components ass soon in Figure 2.



Figure 2. Hardware setup

### 3.3. IP Web Camera

An Internet Protocol Web camera, or IP Web camera, is a sort of advanced digital video camera generally used for observation, and which, not under any condition like basic closed circuit TV (CCTV) cameras, can send and get information by methods for a computer network and the Internet. Although most cameras that do this are webcams, the term IP camera or net cam is regularly connected just to those used for observation that can be directly over to over a system connection.

An IP camera is commonly brought together either centralized (requiring a central framework video recorder (NVR) to manage the record, video and alert organization or decentralized (no NVR required, as camera can record to any area or remote accumulating media). The primary bound IP camera was Axis Net eye 200, released in 1996 by Axis Communications. IP cameras are normally accessible at resolutions from 0.3 (VGA determination) to 29 megapixels. Following is the description provided for IP web camera ass soon in Figure 3.



Figure 3. IP web camera

### 3.4. Raspberry Pi

Raspberry pi board is utilizing the ARM (Advanced Reduced Instruction Set Computing Machine) Technology. ARM technology utilized on the board reduces the cost, heat and power utilization. Following is the description provided for Raspberry pi Board ass soon in Figure 4.



Figure 4. Raspberry pi board

Raspberry pi board is multi center CPU executed as System-on-chip (SoC) weighing 50gm and works on 5V, 700mA power rating. Raspberry pi accessible in 3 models like A, B, B+. the B+ pi board is advanced most recent edition among them, and it keeps running on ARM11 processor with 512MB RAM working at 700MHz frequency. It has SD card for booting operating system like Raspbian, Noobs. It has GPIO pins for accessing Wi-Fi connector, mouse, laptop and so forth Raspberry pi can be utilized as a part of numerous applications.

We have used Raspberry PI in proposed approach as key computational device. It performs email-sending process. It brings the signal from webcams and Raspberry pi send capture pictures to Home owner through email process.

### 3.5. Proposed Algorithm for Security Alert System

In Figure 5 Proposed algorithm explains that camera status and mail subject is passed to pi and checks, if the previous registered member and current live video member match then by giving alert of access it exists. If in case the previous and current video doesn't matches then an alert of access denied email is send to the owner so that owner can take appropriate action.

```

Input : IND, C, Sm
Output : Email
MR = GPIO input (i/p no of Socket)
If RI= Ci then
    Return exit
Else
    Capture video (mobile webcam)
    Attach = SN(USB)
    Sendmail (Message M, Receiver Io, Text To, live video capture)
    Alert door denied!!!!!!
    Take Action(owner)
Endif

```

Figure 5. Algorithm for security alert system

Following is the description for algorithm symbols,

#### 4. RESULTS AND ANALYSIS

In this section result of this work is been explained. Figure 6 scenario provides the webpage to register member, which will be store in the database for future match. Figure 7 scenario provides the webpage to register member, which will be store in the database for future match. Figure 8 scenario provides filling details of family member and start the camera to save the image in the database.

- IND- Intruder detection
- C - Camera Status
- Sm - Message Subject
- MR - Member Registration
- Email - Email of live video
- SN - No. Of Socket pins

Figure 6. Symbol description

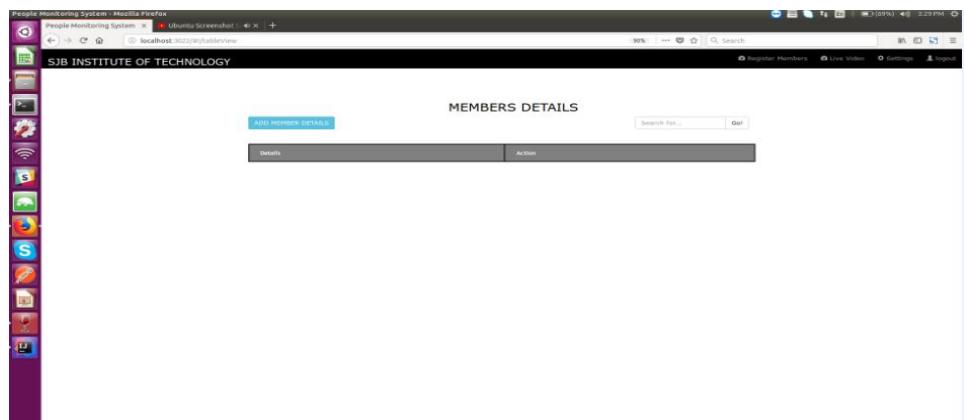


Figure 7. Member details

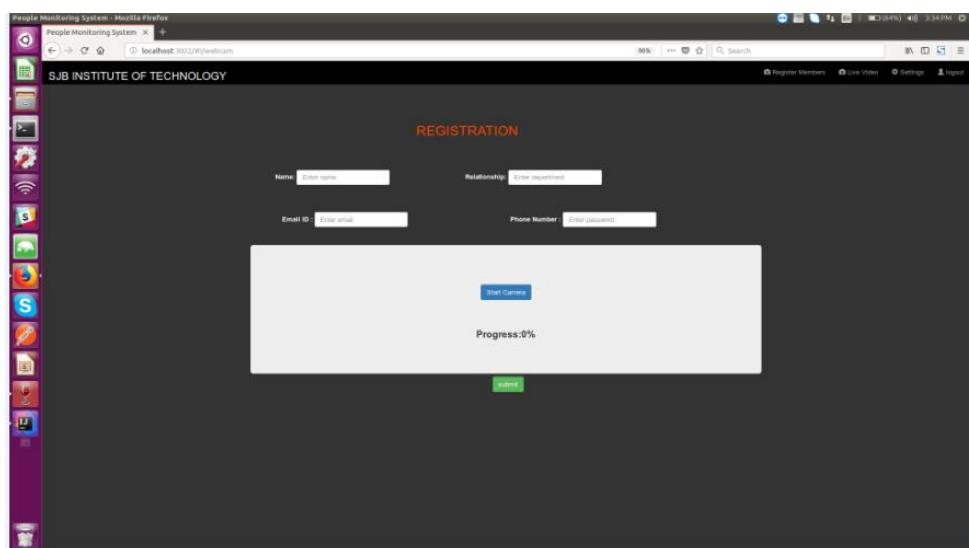


Figure 8. Registration

Figure 9 explains about capturing image once the details are filled. Figure 10 scenario says about Email alert send to the owner, in the case when previous and current registered details does not match so that owner can take appropriate action.

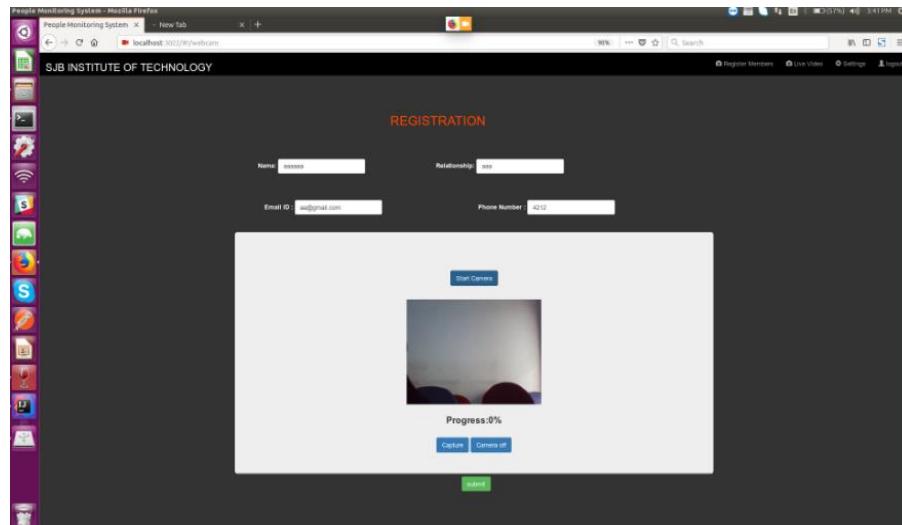


Figure 9. Image Capture

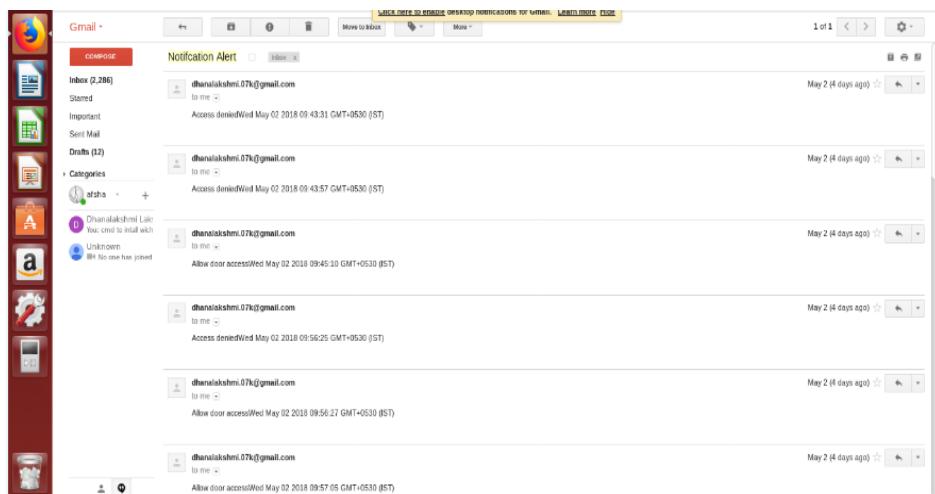


Figure 10. Email alert

## 5. CONCLUSION

In this paper, an enhanced IoT based Security Alert System for Smart Home is designed keeping in mind the end goal to address the issues of minimal effort home security and checking framework utilizing Raspberry pi. These frameworks identify an intruder or any unusual occasion happen in home when no one is accessible in home by sending email caution to owner. Proposed framework presents fundamental level of home security and remote observing likewise affirms the upside of Pi and adaptability regarding expense and its use. This ease security framework has less delay during procedure of sending email.

## 6. FUTURE WORK

We have a plan of designing a system where when the pi encounter an intruder or any unusual event in the home in the absence of owner the door should automatically lock and alert must be received to owner.

**REFERENCES**

- [1] Poonam Gupta, D D Shah, K V V Satyanarayana, "An IoT Framework for Addressing Parents Concerns about Safety of School Going Children", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 6, No. 6, 3052-3059, 2016.
- [2] S. Tanwar, P. Patel, K. Patel, S. Tyagi. "An Advanced Internet of Thing based Security Alert System for Smart Home", Fordham University, USA, 978-1-5090-5957-7/17/\$31.00 2017 IEEE.
- [3] Farrukh Shahzad "Low-Cost Intruder Detection and Alert System Using Mobile Phone Proximity Sensor", Department of Computer Science National University of Computer and Emerging Sciences Islamabad, Pakistan 978-1-5090-3310-2/17/\$3.00 ©2017 IEEE".
- [4] Vishal Jain "IoT Based Smart Security and Home Automation System", Department of Electronics and Communications Engineering National Institute of Technology, Warangal, *International Conference on Computing, Communication and Automation (ICCCA2016)*".
- [5] Raspberry Pi Foundation, <http://www.raspberry.org>
- [6] K. Balasubramanian "Analysis of Remote Control Techniques Employed in Home Automation and Security Systems", 0098 3063/09/\$20.00 © 2009 IEEE.
- [7] Akshat Jain, Shraddha Basantwan, OwaisKaz, Yogita Bang "Smart Surveillance Monitoring System", Computer Engineering Department Pune Institute of Computer Technology Pune, India, 2017 *International Conference on Data Management, Analytics and Innovation (ICDMAI) Zeal Education Society*, Pune, India, Feb 24-26, 2017".
- [8] Ayush Panwar, Anandita Singh, "Eyrie Smart Home Automation using Internet of Things", Dept. of Electronics & Comm. Engg. Manipal University Jaipur, India *Computing Conference 2017* 18-20 July 2017. London, UK.
- [9] Robles, Rosslin John, et al. "A review on security in smart home development." *International Journal of Advanced Science and Technology* 15 (2010).
- [10] Supreeta Venkatesan "Design and Implementation of an automated Security System using Twilio Messaging Service", 2017 *International Conference on Smart Cities, Automation and Intelligent Computing Systems yogyakarta, Indonesia*, November 08-10, 2017".
- [11] Shaik Anwar and D. Kishore," IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone", *International Journal of Engineering Research & Technology (IJERT)*, 5(12), 2016, pp. 1-5.